CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A method of performing a reduction operation in a cryptographic calculation in a digital computer, the method comprising:

selecting a modulus having a first section with a plurality of "1" Most ~~Significant~~ Significant Word states and a second section which further comprises: a~~,~~ plurality of "1" or "0" states whereby ~~the~~ a number formed of the two sections is a modulus ~~or a multiple of a modulus,~~; and

operating a reduction operation on the ~~modulus/multiple~~ modulus comprising:

multiplying a first variable $n_{0'}$ by a second variable r_3 to produce a first result;

adding the first result to a third variable r_1 and a fourth variable Br_2 to produce a first sum;

dividing the first sum into an upper half and a lower half;

multiplying the upper half by the first variable $n_{0'}$ to produce a second result;

adding the second result to the lower half and a fifth variable r_0 to produce a second sum, thereby permitting use of the second sum as the modulus.

2. (Currently Amended) A method according to claim 1, further comprising:

effecting a plurality of multiplication operations.

3. (Currently Amended) A method according to claim 2, further comprising:

effecting a plurality of multiplication operations followed by effecting a reduction operation.

4. (Currently Amended) A method according to claim 3, further comprising:

repeating the combined multiplication operations and reduction operation.

5. (Currently Amended) A method according to claim 1, further comprising:

using a multiple of the ~~modulus/multiple~~ modulus.

6. (Currently Amended) A method according to claim 1,

wherein, when ~~the~~ a last multiplication gives an overflow, the overflow is added to a part of ~~the~~ a selected number.

7. (Currently Amended) A method according to claim 6, wherein, when the overflow addition step produces an overflow, then the first variable n_0' is added to the overflow.

8. (Currently Amended) A method according to claim 1, wherein ~~the~~ a carry c between two adjacent multiplications is effected as ~~the~~ an addend in the next multiplication.

9. (Currently Amended) A method according to claim 1, further comprising:

monitoring the number of leading "1"s to determine if the number is less than (k-2).

10. (Currently Amended) A method according to ~~claim 6~~ claim 9, further comprising:

initiating ~~the~~ a next calculation when the number of leading "1"s is less than (k-2).

11. (Currently Amended) A method according to claim 1, the method further comprising:

operating 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits.

12. (Currently Amended) A method according to claim 1, the method ~~comprises~~ further comprising:

operating 128-bit ECC and a word size of 64-bit,

the modulus comprises a first section of 74 bits and a second section of 54 bits.

13. (Currently Amended) A method according to claim 1, the method further comprising:

operating 256-bit ~~ECG~~ ECC and a word size of ~~54 bit~~ 64-bit,

the modulus comprises a first section of 202 bits and a second section of 54 bits.

14. (Currently Amended) A computer program product directly loadable into the internal memory of a digital computer, comprising:

software code portions for performing the method of claim 1

when said product is run on a computer.

15. (Currently Amended) A computer program directly ~~load able~~ loadable into the internal memory of a digital computer, comprising:

software code portions for performing the method of claim 1 when said program is run on a computer.

16. (Canceled).

17. (Canceled).

18. (Currently Amended) An apparatus that performs ~~Apparatus for performing~~ a reduction operation in a cryptographic calculation on a digital computer, the apparatus comprising:

a plurality of input registers that store a plurality of input operands;

a plurality of output registers that store a plurality of outputs; and

a multiplier that produces said outputs using a function that operates on variables from both said input registers and said output registers;

wherein said multiplier ~~means to select~~ selects a modulus ~~or a multiple of a modulus~~ having a first section with a plurality of "1" states and a second section having a plurality of "1" or "0" states whereby ~~the~~ a number formed of the two sections is a modulus ~~or a multiple of a modulus, and means for operating~~ performs a reduction operation on the~~ modulus/multiple~~ modulus, the reduction operation comprising:

multiplying a first variable $n_{0'}$ by a second variable r_3 to produce a first result;

adding the first result to a third variable r_1 and a fourth variable Br_2 to produce a first sum;

dividing the first sum into an upper half and a lower half;

multiplying the upper half by the first variable $n_{0'}$ to produce a second result; adding the second result to the lower half and a fifth variable r_0 to produce a second sum, thereby permitting use of the second sum as the modulus.

19. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18, further comprising:

means to effect a plurality of multiplication operations.

20. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 19, further comprising:

means to effect a plurality of multiplication operations followed by a reduction operation.

21. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 20, further comprising:

means to repeat the ~~combined~~ plurality of multiplication operations and the reduction operation.

22. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18, further comprising: means ~~(10-17)~~ to use a multiple of the ~~modulus/multiple~~ modulus.

23. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18, further comprising:

means, when ~~the~~ a last multiplication gives an overflow, to add the overflow to a part of ~~the~~ a selected number.

24. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 23, further comprising:

means, when the overflow addition step produces an overflow, to add the first variable n_0' ~~n.sub.0~~' to the overflow.

25. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18, further comprising:

means to effect ~~the~~ a carry c between two adjacent multiplications as ~~the~~ an addend in the next multiplication.

26. (Currently Amended) Apparatus according to claim 18, further comprising:

means to monitor the number of leading "1"s to determine if the number is less than (k-2).

27. (Currently Amended) ~~Apparatus according to claim 18~~

The apparatus of claim 26, further comprising:

means to initiate ~~the~~ a next calculation when the number of leading "1"s is less than (~~K-2~~ k-2).

28. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18, further comprising:

with means for 192-bit ~~EEC~~ ECC and a word size of 64-bit,

the modulus comprises a first section of 74 bits and a second section of 54 bits.

29. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18,

further comprising:
with means for 128-bit ECC and a word size of 64-bit,
the modulus comprises a first section of 74 bits and a second section of 54 bits.

30. (Currently Amended) The apparatus of ~~Apparatus according to~~ claim 18, further comprising:
with means, for 256-bit ECC and ~~81~~ word size of 64-bit,
the modulus comprises ~~81~~ first section of 202 bits and ~~81~~ second section of 54 bits.

31. (Canceled).

32. (Canceled).

33. (Canceled).